UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/718,734	11/22/2000	George M. Brookner	770P009595-US(PAR)	2840

2512 7590 06/02/2005

PERMAN & GREEN
425 POST ROAD
FAIRFIELD, CT 06824

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 06/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/718,734	BROOKNER ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20 and 22-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20 and 22-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *08/16/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in replay to an amendment filed on October 14, 2004 and an response to Election/restriction made on March 10, 2005.

Claims 1, 2, 13-14, 22, 27 and 30 have been amended and claim 21 have been cancelled on the first amendment filed on October 14, 2004 and on March 10,2005 applicant elected Claims 1-20 and 22-26 in response to Election/restriction.

Claims 1-20 and 22-26 are pending in the application.

Response to Argument

2. Applicant's remark/arguments filed on October 14, 2004 have been fully considered but they are not persuasive.

Applicants first argument is based on the prior art used in rejection namely Kuhn. Applicant argued that the references on the record namely Kuhn does not teach PIN creation. **In response to applicant's argument** that the reference/Kuhn fail to teach Pin creation, the examiner disagrees with the argument and points out the figure on the last page shows how pin are calculated for EuroCheque ATM Debit Cards which is analogous to the pin creation and Kuhn also discloses elements that meets most of the limitation of the claims.

Applicant second argument is refereeing to the prior art used in rejection namely the combination of Kuhn and Matyas. Applicant argued that the combination does not disclose generating a number of random binary bits. Applicant further argued that there is nothing in the Kuhn's process related to phenomenon that does not produce the same outcome or consequences every time it occurs under identical circumstances. Furthermore, there is nothing in Kuhn that provides a sample drawn from a population so that each member of the population has equal chance to be drawn. Thus Kuhn does not describe generating a number of random binary bits.

Examiner disagrees with this argument.

Examiner would point out that Kuhn discloses the method wherein the number of bits is sixty-four (64-bit pattern) or which is equivalent to the 16-digit decimal number.(page 1,lines 12-15; figure on the last page).Kuhn discloses that the 64 bits pattern or its equivalent 16-digit decimal number is formed by concatenating five digits of the bank routing number, ten digit account number which is the unique number for each customer, and a single digit card sequence number and after that the result was encoded (encrypted) using the DES algorithm with the secret 56-bit institute key k1.(page1, lines 12-17; figure on the last page).This will make each successive digit or bits to be equally likely and unpredictable to meet the recitation of Random. It is not only true that each bits are equally likely but also true that they are used in calculation creating a pin which has to be unique for each customers.

Applicant third argument is refereeing to the limitation in claim 1. Applicant argued that there is nothing in the combination of Kuhn and Matyas related to determining the least significant bits of the number of bits. Applicant argued that the examining 4 specific digits, of a hexadecimal number is different from determining the least significant bits of number of bits because the specified digits do not necessary include all of those in a least significant position and hexadecimal number by definition is not a binary format.

Examiner disagrees with this argument.

Examiner points out that Kuhn discloses determining /selecting any 4 arbitrary hexadecimal digits out of the 16 hexadecimal digit (take 3-6 hexadecimal digits) meets the limitation of determining the least significant bits because taking 3-6 digits or its equivalent 4 hexadecimal digit or its equivalent 16 bits out of the 16 hexadecimal digit or its equivalent 64 bits is an arbitrary design choice. Selection the right most, or the middle or the left most bits is arbitrary design choice. Therefore what is described by

Kuhn meets the recitation of sixteen least significant bits.(page 1, lines 17, page 4; figure on the last page). In response to the argument that hexadecimal number by definition is not a binary format Examiner would point that the fact that hexadecimal format is not written in the binary format does not patentably distinguishes the limitation from what is disclosed by Kuhn. In fact converting hexadecimal to its equivalent binary format or vice-versa is known to a person skilled in the art.

Applicant forth argument is refereeing to the limitation in claim 1. Applicant argued that Kuhn does not disclose or suggest converting the least significant bits to a decimal integer.

Examiner disagrees with this argument

Examiner would point out that Kuhn discloses, Converting the hexadecimal digit (3-6) in to a decimal integer using a decimalization mapping (Figure on the last page)(this meets the limitation of converting the least significant bits to a decimal integer). As it is already discussed above it has been shown why the least significant bits is equivalent to what is disclosed by the prior art. Therefore by the same analogy, this particular limitation is also disclosed by Kuhn.

Applicant's fifth argument is regarding the claims 13-19 and 25.

Applicants argued that the since the independent claims 13 which recites all the limitation of claim 1 are patentable therefore claim 13 and all the claims dependent thereon are also in condition for allowance for the same reasons argued for the independent claims 1.

In response to the above argument by the applicant, the examiner response discussed to the independent claims 1 mentioned above is also valid towards this argument.

Applicant last argument is regarding the dependent claims 20 and 22-24.

Applicants argued that the since the independent claims 13 which recites all the limitation of claim 1 are patentable therefore all the claims dependent thereon are also in condition for allowance for the same reasons argued for the independent claims 1.

Examiner disagrees with the above argument.

In response to the above argument by the applicant, the examiner response discussed to the independent claims 1 mentioned above is also valid towards this argument.

Therefore all the **elements of the limitations of claims** are explicitly or implicitly or inherently suggested and disclosed by the references on the records.

The rejections remains to be valid unless and otherwise the claims are further amended to introduce/include some elements of the application with out adding new matters and that are not taught/described/suggested/disclosed by the references on the record.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-12** are rejected under 35 U.S.C. 103(a) as being unpatentable over Markus G. Kuhn (hereinafter refereed to as Kuhn) (reference U)(07/30/1997) in view of Matyas et al (hereinafter refereed to as Matyas)(U.S. Patent No. 4,924,514).

5. **As per claim 1**, Khun teaches a method for generating PIN comprising: Generating a number of random binary bits (this number is transferred in to a 64-bit pattern and meets the limitation of random bits);(Page 1, lines 12-17; figure on the last page)

Determining any arbitrary digits out of the 16 hexadecimal digit (take 3-6 hexadecimal digits), (meets the limitation of determining the least significant bits).(page 1, lines 17, page 4; figure on the last page)

Converting the hexadecimal digit (3-6) in to a decimal integer using a decimalization mapping (Figure on the last page)(this meets the limitation of converting the least significant bits to a decimal integer).

Furthermore Kuhn teaches shifting the values of the integer by a predetermined (selected) constant to produce a shifted integer (constant is an offset in the reference) (figure on the last page).
Kuhn does not explicitly teaches encoding the shifted integer as bits in a PIN block in accordance with a standard. ("standard" is understood by the examiner to be "ISO 9564-1").
However Matyas teaches encoding the pin in a pin block in accordance with one of the several industry-accepted de facto standard.(standard could be ISO 9564-1)(column 7,lines 52; column 5, lines 53-55 and column 5, line 63-67).

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the encoding of the pin in the pin block according to the standard as per teachings of Matyas in to the method of generating Pin as taught by Kuhn in order to produce PIN with the PIN block satisfying or in accordance to the industry accepted de facto standard (standard could be ISO 9564-1)

6. **As per claim 2**, the combination of khun and Matyas teach the method as applied to claim 1 above. Furthermore, Matyas teaches the method wherein the shifted integer is encoded in accordance with encoding standard 9564-1(column 5,line 65-68 and column 6, line 1).

7. **As per claim 3**, the combination of Kuhn and Matyas teach the method as applied to claim 1 above. Furthermore, Kuhn teaches the method wherein the number of bits is sixty-four (64-bit pattern) or which is equivalent to the 16-digit decimal number.(page 1,lines 12-15; figure on the last page).Kuhn discloses that the 64 bits pattern or its equivalent 16-digit decimal number is formed by concatenating five digits of the bank routing number, ten digit account number, and a single digit card sequence number and after that the result was encoded (encrypted) using the DES algorithm with the secret 56-bit institute key k1.(page1, lines 12-17; figure on the last page).(this will make each successive digit or bits to be equally likely and unpredictable to meet the recitation of Random.)

8. **As per claim 4,** the combination of Kuhn and Matyas teach the method as applied to claim 1 above. Furthermore, Kuhn teaches the method wherein the number of bits are sixteen or (4 decimal integer).(taking 3-6 digits or its equivalent 4 decimal integer).(page 1, lines 17). selecting any sixteen bits out of the 64 bits or any 4 hexadecimal digit out of the 16 hexadecimal digit is arbitrary. Selection the right most, or the middle or the left most bits is arbitrary. (Khun disclosure meet the recitation of sixteen least significant bits

9. **As per claim 5**, the combination of Kuhn and Matyas teach the method as applied to claim 1 above. Furthermore Kuhn teaches the method wherein the constant is the offset 1707). (figure on the last page). Kuhn also discloses replacing the 1st digit by 1, if the first of those digits is a 0, to make sure that the leading digit is not equal to 0.(page 1, line 18; figure on the last page)(This meets the recitation for the constant.

10. **As per claim 6-11** the combination of kuhn and Matyas teach the method as applied to claim 1 above. Furthermore Matyas teaches the method wherein the PIN block includes the PIN block formats which have been standardized or have become industry-accepted de facto standards.(standard could be ISO 9564-1)(column 5,lines 63-68; column 6,lines 1-19 and column 7,line 53).

11. **As per claim 12**, the combination of kuhn and Matyas teach the method as applied to claim 1 above. Furthermore Kuhn teaches the method wherein the number of bits is sixty-four (64-bit pattern) or which is equivalent to the 16-digit decimal number.(page 1,lines 12-15; page4(last page)).Kuhn also teaches that bits or its

equivalent 16-digit decimal number is formed by concatenating five digits of the bank routing number, ten digit account number, and a single digit card sequence number and finally the result was encoded (encrypted) using the DES algorithm with the secret 56-bit institute key.(page1, lines 12-17; page 4).(This will meet the recitation of pseudorandom generation).

12. Claims **13-19, 25-26** are rejected under 35 U.S.103(a) as being unpatentable over Markus G. Kuhn (hereinafter refereed to as Kuhn) (reference U)(07/30/1997) in view of Matyas et al (hereinafter refereed to as Matyas)(U.S. Patent No. 4,924,514) further in view of Holch et al. (hereinafter refereed to as Holch) (U.S. Patent No. 6,280,328)

13. As per claim **13 and 20** Kuhn discloses a method for managing security of a PIN used to provide access to a secure device, comprising:

Khun teaches a method for generating/choosing PIN comprising:

Generating a number of random binary bits (this number is transferred in to a 64-bit pattern and meets the limitation of random bits);(Page 1, lines 12-17; figure on the last page)

Determining any arbitrary digits out of the 16 hexadecimal digit (take 3-6 hexadecimal digits), (meets the limitation of determining the least significant bits).(page 1, lines 17, page 4; figure on the last page)

Converting the hexadecimal digit (3-6) in to a decimal integer using a decimalization mapping (Figure on the last page)(this meets the limitation of converting the least significant bits to a decimal integer).

Furthermore Kuhn teaches shifting the values of the integer by a predetermined (selected) constant to produce a shifted integer (constant is an offset in the reference) (figure on the last page).

Kuhn does not explicitly teaches encoding the shifted integer as bits in a PIN block in accordance with a standard. ("standard" is understood by the examiner to be "ISO 9564-1") and Khun also does not teach communicating the PIN to a user of the device via a first communication channel separate and apart from a second communication channel used to provide the device to the user.

However Matyas teaches encoding the pin in a pin block in accordance with one of the several industry-accepted de facto standard.(standard could be ISO 9564-1)(column 7,lines 52; column 5, lines 53-55 and column 5, line 63-67). Matyas also discloses communicating the PIN to a user of the cardholder via a communication channel (mail) separate and apart from a channel used to provide the card (device) to the user.(figure 5, column 4, lines 57-62).

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the encoding/communicating of the pin as per teachings of Matya's in to the method of generating Pin as taught by Kuhn in order to produce PIN with the PIN block satisfying or in accordance to the industry accepted de facto standard (standard could be ISO 9564-1) and communicate the Pin securely.

The combination of Kuhn and Matyas does not disclose

storing an encrypted version of the PIN in the device.

However, In the same field of endeavor **Holch** discloses

choosing the PIN;(column 6, 20-21) and

storing an encrypted version of the PIN in the device;(column 6,21-24) and

Furthermore Holch teaches communicating PIN to the account server after encrypting the PIN (column 7,lines 16-19)

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the storing of encrypted version of the pin in the device as per teachings of Holch in to the method as taught by the combination of Kuhn and Matyas in order to ensure that the PIN is delivered to the actual user safely and securely.

14. **As per claim 14,** the combination of Khun Matyas and Holch teach the method as applied to claim 13 above. Furthermore Matyas teaches the method wherein the standard said communication channel is a secure channel.(figure 5, column 4, lines 57-62)

15. **As per claim 15**, the combination of Khun Matyas and Holch teach the method as applied to claim 14 above. Furthermore Matyas teaches the method comprising using encryption to render said communication channel secure.(figure 5; column 4, lines 57-62).

16. **As per claim 16**, the combination of Khun Matyas and Holch teach the method as applied to claim 13 above. Furthermore Matyas teaches the method wherein the user of said device chooses said PIN.(column 6, line 20-21).

17. **As per claim 17**, the combination of Khun Matyas and Holch teach the method as applied to claim 16 above. Furthermore Holch teaches a method wherein a

manufacturer of said device causes said encrypted version of said PIN to be stored in said device.(column 6,21-24).

18. **As per claim 18 and 19** the combination of Khun Matyas and Holch teach the method as applied to claim 17 above. Furthermore Holch teaches the method further comprising the manufacturer or the card (device) issuer storing a record of said PIN in the Account server(column 6, lines 29-31). Therefore It is also obvious for one having ordinary skill in the art at time of the invention to consider that the card (device) issuer has a capability of discarding all the records of said PIN if it has the capacity of storing a record of PIN.

19. **As per claim 25 and 26** the combination of Khun Matyas and Holch teach the method as applied to claim 13 above. Furthermore Holch teaches the method wherein the said device (magnetic card) stores the value of funds.(colum 6, 37-44).

20. **As per claim 22**, the combination of Khun Matyas and Holch teaches the method as applied to claim 13 above. Furthermore Holch teaches a method wherein a manufacturer of said device causes said encrypted version of said PIN to be stored in said device.(column 6,21-24).

21. **As per claim 23 and 24** the combination of Khun Matyas and Holch teaches the method as applied to claim 22 above. Furthermore Holch teaches the method further comprising the manufacturer or the card (device) issuer storing a record of said PIN in the Account server(column 6, lines 29-31). Therefore It would have been obvious for

one having ordinary skill in the art at time of the invention was made to consider that the card (device) issuer has a capability of discarding all the records of said PIN if it has the capacity of storing a record of PIN.

Conclusion

22. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

SL

May 25, 2005

JUSTIN T. DARROW
PRIMARY EXAMINER